Office Action Summary	Application No.	Applicant(s)	
	09/580,689	MARIA, ARTURO	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-14,23-30 and 32-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-14, 23-30, and 32-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 6/19/2007, Applicant amends claim 1 to more clearly recites the invention as supported in the specification, the 112th rejection first paragraph is withdrawn in view of the amendment. In communications filed on 6/19/2007, claims 1, 23, and 30 have been amended. The following claims 1-5, 7-14, 23-30, and 32-43 are pending and are presented for examination.

1.1 Applicant's arguments, pages 9-15, filed on 6/19/2007, with respect to the rejection of claims 1-5, 7-14, 23-30, and 32-43 have been fully considered but they are not persuasive. With respect to claim 1, claim 1 has been amended to more particularly point out Applicant's invention as supported by the specification. With respect to claims 1 and 23, in response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, providing a server for sending request to a software agent to access other remote devices would allow the agent to perform task at critical moment when attack is detected as suggested by **Lavian et al** (column 3, lines 22-50). In addition, KSR forecloses the argument that a specific

teaching suggestion or motivation is required to support a finding of obviousness. See the recent Board decision *Ex parte Smith,* --USPQ2d--, slip op. at 20, (BD. Pat. App. & Interf. June 25, 2007) citing KSR, 82 USPQ2d at 1396) (available at "http://www.uspto.gov/web/offices/dcom/bpai/prec/fd071925.pdf"). Examiner asserts that the claims as amended are still rendered obvious over the prior art. No specific arguments have been provided with respect to Lavian and Examiner asserts that Lavian provides the deficiencies found in Yavatkar. With respect to claim 23, applicant generally alleges that nothing in these references suggests software agents that are executing on the plurality of computers when they receive a request for installation of intrusion detection software (see for instance Lavian column 7, lines 60-65 disclosing that agent can already be resident in the computer. Regarding dependent claims 5, 11, 12, and 41-43, Applicant argues about the combination of references. Applicant's arguments regarding the combination of references are not persuasive as explained above. Applicant adds "the so-called stop condition" of Yavatkar is not a stop condition.

Examiner respectfully disagrees as Yavatkar discloses "stop execution". Regarding dependent claims 26 and 39-40. In response to applicant's argument that Brown discloses the use of time to accommodate bandwith limitations, the fact that applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985. Therefore as indicated above, applicant has not overcome the rejection in view of the prior art . A new ground of rejection is set forth below as necessitated by the amendment in view of the same prior art.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 7-10, 13-14, 23-25, 27-30, and 32-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,735,702 to **Yavatkar et al** in view of US Patent 6,842,781 to **Lavian et al**.

As per claim 1, Yavatkar et al discloses a method for implementing an intrusion detection system in a network, comprising receiving notification to initiate intrusion detection software as watchdog agents on a plurality of remote computers (see column 16, lines 17-30 and column 14, lines 18-28) that meets the recitation of *receiving a request at a software agent program to initiate intrusion detection services on a plurality of remote computers* request may be issued by administrator or any monitoring software residing on any computer, wherein the request is issued in response to a notification of a network intrusion (see column 16, lines 17-30) that meets the recitation of *wherein the request is issued in response to a notification of a*

network intrusion; and discloses the launching of mobile agents on nodes which also can install code into the device (see column 14, lines 18-28) that meets the recitation of *installing intrusion detection software on said remote computer via said software agent program*, and executing other agents on the remote computers (see column 14, lines 49-63) that meets the recitation of *executing said intrusion detection software on said remote computer via said software agent program*, for example (see page 165, first column and conclusion). See also embodiment in column 18, lines 32-55. **Yavatkar et al** is silent about the request is received from a server. **Lavian et al** in an analogous art teaches method and system for performing a network management by executing the network management application at a software agent installed on each of a plurality of network devices for performing the task (see column 3, lines 22-27 and lines 47-50). The method includes receiving request from the NMS server at a software agent installed on each of a plurality of network devices to perform the task on each respective one of the one or more network devices (plurality of computers) (see column 7, lines 43-45 and column 3, lines 23-27 and col. 9, lines 44-46) and installing and executing the software on the one or more computers (via a software agent residing at each device col. 9, lines 44-46) in response to the request (see column 7, lines 50-67 and column 3, lines 22-27 and lines 47-50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Yavatkar et al** method of using a watchdog agent for launching agent when a particular network condition is detected to provide a server for requesting the software installation at one or more network devices having a software agent because it would allow the agent to perform task at critical moment when attack is detected as suggested by **Lavian et al** (column 3, lines 22-50).

As per claim 2, the combination of references discloses proactive environment can exist on each of the multiple nodes and can create agents and enable mobile agents to start, suspend, stop, and destroy services (see column 5, lines 8-20) that meets the recitation of receiving a request to terminate intrusion detection services at said software agent program and as disclosed by **Lavian et al** manager server may control agents and requests them for performing tasks (see **Yavatkar et al** column 7, lines 43-50).

As per claim 3 the combination of references discloses the limitation of monitoring for fulfillment of a stop condition (see **Yavatkar et al** column 5, lines 8-20).

As per claims 4 and 13, the combination of references discloses wherein said stop condition is based on network traffic conditions (see **Yavatkar et al** column 18, lines 36-37).

As per claim 7, the combination of references discloses deployed watchdog agents at multiple nodes at key points such as routers that meets the recitation of selecting said remote computers from a plurality of eligible computers (see **Yavatkar et al** column 14, lines 18-28).

As per claim 8, the combination of references discloses resources to be accessed may be based on routing table that meets the recitation of said selecting step is accomplished based on a network map (**Yavatkar et al** column 14, lines 10-17).

As per claim 9, the combination of references discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (see **Yavatkar et al** column 5, lines 30-36 and column 10, lines 26-42).

As per claims 10 and 14, the combination of references discloses controlling method for querying for agents including to ensure integrity of agents they should be verified using a cryptographic authentication scheme that meets the limitation of wherein said request is verified using a cryptographic authentication scheme (see **Yavatkar et al** column 10, lines 43-52 and column 9, lines 52-67).

As per claim 23, Yavatkar et al substantially discloses a system for detecting intrusions in a computer network comprising: *a plurality of computers executing software agents* (see column 8, lines 11-20); *an intrusion detection server* (see column 1, lines 21-25) any network device can be acted as an instruction server without departing from the spirit and scope of the invention disclosed by **Yavatkar et al**; and discloses an access control list with all the access rules (see column 10, lines 26-42) that meets the limitation of a database configured to store at least one rule defining at least one response to a network intrusion, wherein said intrusion detection server is configured to send a request to execute intrusion detection software to software agents at a plurality of computers (see column 14, lines 18-28) when intrusion detection services are needed based on the at least one rule stored in said database (see column 10, lines 26-52 and column 14, lines 44-48). **Yavatkar et al** is silent about the request is received from a server. **Lavian et al** in an analogous art teaches method and system for performing a network

management by executing the network management application at a software agent installed on each of a plurality of network devices for performing the task (see column 3, lines 22-27 and lines 47-50) and also discloses a database to facilitate converting object oriented requests for MIB information into requests for network parameters (see column 5, lines 35-53); and a network table including a list of network addresses associated with network devices to assist in requests from the network management application (see column 6, lines 16-27). The method includes receiving request from the NMS server at a software agent installed on each of a plurality of network devices to perform the task on each respective one of the one or more network devices (plurality of computers) (see column 7, lines 43-45 and column 3, lines 23-27 and col. 9, lines 44-46) and installing and executing the software on the one or more computers (via a software agent residing at each device col. 9, lines 44-46) in response to the request (see column 7, lines 50-67 and column 3, lines 22-27 and lines 47-50) to initiate detection service on each of the computers or network devices executing the software agents (see column 7, lines 43-59; column 3, lines 22-27 and lines 47-50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Yavatkar et al** method of using a watchdog agent for launching agent when a particular network condition is detected to provide a server for requesting the software installation at one or more network devices having a software agent because it would allow the agent to perform task at critical moment when attack is detected as suggested by **Lavian et al** (column 3, lines 22-50).

As per claim 24, the combination of references discloses calling for more agents when network intrusion is detected that meets the recitation of wherein said intrusion detection server

increases the number of said plurality of computers executing intrusion detection software when a network intrusion is detected (see **Yavatkar et al** column 19, lines 14-20).

As per claim 25, the combination of references discloses the limitation of wherein said intrusion detection server changes the number of said plurality of computers executing intrusion detection software when the level of network traffic changes (see **Yavatkar et al** column 19, lines 14-20).

As per claim 27, the combination of references discloses the limitation of wherein said database contains information about the plurality of computers (see **Yavatkar et al** column 10, lines 26-42).

As per claim 28, the combination of references discloses the limitation of wherein said information includes a map of said computer network (see **Yavatkar et al** column 5, lines 21-36).

As per claim 29 the combination of references discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (see **Yavatkar et al** column 5, lines 30-36 and column 10, lines 26-42).

As per claim 30, Yavatkar et al substantially discloses a method for implementing an intrusion detection system in a network, comprising in one embodiment the watchdog agent

receives notification from the bloodhound agent, (see column 16, lines 17-30; column 18, lines 31-40 and lines 49-55) that meets the recitation of *receiving notification of a network intrusion;*

In response to the notification, the watchdog agent launches an agent or installing intermediate filters in the network (see column 18, lines 54-64) that meets the recitation of *transmitting an installation request in response to the notification* for example (see column 18, lines 49-64), installing intermediate filters in the network (see column 18, lines 62-67) to combat attacks the present invention may find paths and take appropriate actions such as installing firewall entries at the appropriate devices to block such traffic (see column 14, lines 10-17) that meets the recitation of *installing intrusion detection software on said remote computer via said software agent program in response to the request.* **Yavatkar et al** even discloses a network may have with multiple gateways and when a particular gateway is identified for allowing traffic filter is installed on that particular gateway to halt traffic (see column 13, lines 54-58). As interpreted by the Examiner the several filters in the network may be installed in more than one device, since the attack is taken through different paths. **Yavatkar et al** further discloses when such a path is found appropriate action may be installing firewall entries at the appropriate devices to block traffic (see column 14, lines 10-17). In another embodiment, agents are being requested and deployed in notification of a network intrusion (see column 14, lines 18-28). **Yavatkar et al** is silent about the request is received from a server. **Lavian et al** in an analogous art teaches network and system for performing a network management by executing the network management application at a plurality of network devices or agent for performing the task (see column 3, lines 22-27 and lines 47-50). The method includes transmitting a software installation from the server to one or more network devices (plurality of computers) (see column 7, lines 43-

45 and column 3, lines 23-27) and installing the software on the one or more computers (via a software agent residing at each device col. 9, lines 44-46) in response to the request (see column 7, lines 50-67 and column 3, lines 22-27 and lines 47-50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Yavatkar et al** method of using a watchdog agent for launching agent when a particular network condition is detected to provide a server for requesting the software installation at one or more network devices having a software agent because it would allow the agent to perform task at critical moment when attack is detected as suggested by **Lavian et al** (column 3, lines 22-50).

As per claim 32, the combination of references discloses deployed watchdog agents at multiple nodes at key points such as routers that meets the recitation of selecting said remote computers from a plurality of eligible computers (see **Yavatkar et al** column 14, lines 18-28).

As per claim 33, the combination of references discloses resources to be accessed may be based on routing table that meets the recitation of said selecting step is accomplished based on a network map (see **Yavatkar et al** column 5, lines 21-36).

As per claim 34, the combination of references discloses the limitation of wherein said selecting step is accomplished based on a knowledge base (see **Yavatkar et al** column 5, lines 30-36 and column 10, lines 26-42).

As per claim 35, the combination of references discloses controlling method for querying for agents including to ensure integrity of agents they should be verified using a cryptographic authentication scheme that meets the limitation of wherein said request is verified using a cryptographic authentication scheme (see **Yavatkar et al** column 10, lines 43-52 and column 9, lines 52-67).

3. **Claims 5, 11, 12, 36-38, and 41-43** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,735,702 to **Yavatkar et al** in view of US Patent 6,842,781 to **Lavian et al** as applied to claims 1-13 and 23 and further in view of US Patent Publication 2002/0003884 to **Sprunk.**

As per claims 11 and 41, Yavatkar et al discloses a proactive environment that allows agent to operate on one node, stop execution, and resume execution which could be broadly and reasonably interpreted by one of ordinary skill in the art as wherein said request includes a stop condition indicating when to stop executing the intrusion detection software program, for example (see column 5, lines 18-20). **Yavatkar et al** does not explicitly state that the stop condition applies to all eligible computers. **Sprunk** in an analogous art teaches a secure access system comprising an access control processor (ACP) for monitoring which application objects are executed in computer systems and to confirm their authorization and authenticity. Although the exemplary embodiment uses set top boxes, the invention is applicable to PC computers, which are susceptible to viruses, and hackers as disclosed in the background. **Sprunk** discloses that checkpoints are embedded in the applications on each system to trigger the ACP, and among

the features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) and further discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of a stop condition indicating when to stop executing the intrusion detection software program and wherein the stop condition applies to all eligible computers. As interpreted by the Examiner, the execution of the software will stop on all computers with a date/time expiration status. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped in the event that an unauthorized object is detected as suggested by **Sprunk**. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on what applications or objects are authorized to be executed on each computer system.

As per claims 5 and 12, Yavatkar et al does not explicitly state that the stop condition is an expiration time. **Sprunk** in an analogous art teaches a secure access system comprising an access control processor (ACP) for monitoring which application objects are executed in a computer system and to confirm their authorization and authenticity. Although the exemplary embodiment uses set top boxes, the invention is applicable to PC computers, which are susceptible to viruses, and hackers as disclosed in the background. **Sprunk** discloses that checkpoints are embedded in the applications on each system to trigger the ACP, and among the

features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) and further discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of wherein the stop condition is an expiration time. As interpreted by the Examiner, the execution of the software will stop on all computers with a date/time expiration status. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk**. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

As per claims 36 and 37, Yavatkar et al discloses a proactive environment that allows agent to operate on one node, stop execution, and resume execution which could be broadly and reasonably interpreted by one of ordinary skill in the art as wherein said request includes a stop condition indicating when to stop executing the intrusion detection software program, for example (see column 5, lines 18-20). **Yavatkar et al** does not explicitly state that the stop condition is an expiration time. **Sprunk** in an analogous art teaches a secure access system comprising an access control processor (ACP) for monitoring which application objects are executed in a computer system and to confirm their authorization and authenticity. Although the

exemplary embodiment uses set top boxes, the invention is applicable to PC computers, which are susceptible to viruses, and hackers as disclosed in the background. **Sprunk** discloses that checkpoints are embedded in the applications on each system to trigger the ACP, and among the features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) and further discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of a stop condition indicating when to stop executing the intrusion detection software program and wherein the stop condition is an expiration time. As interpreted by the Examiner, the execution of the software will stop on all computers with a date/time expiration status. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Yavatkar et al** to provide a way of monitoring wherein execution of the application can be stopped in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk**. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

As per claim 38, the combination of references discloses wherein said stop condition is based on network traffic conditions (see **Yavatkar et al** column 18, lines 36-37).

As per claim 42, Sprunk discloses a monitoring process wherein checkpoints are embedded in the applications on each system to trigger the ACP, and among the features of the ACP, the ACP can stop running applications if an error is detected or if authorization expires (see paragraph 54) that meets the recitation of monitoring for fulfillment of a stop condition at each of the plurality of remote computers executing intrusion detection software (see paragraphs 5, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application can be stopped at each of the plurality of remote computers because it would allow the software to stop execution in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk** above. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

As per claim 43, Sprunk discloses "Lifetime information allows the expiration of the authorization of the object to prevent use after a certain date and time", and authorization of a software object can be programmed to expire after a certain amount of time (see paragraphs 62 and 66) that meets the recitation of wherein the stop condition for each of the plurality of computers is based on a time during which each of the plurality of remote computers has been executing intrusion detection software (see paragraphs 5, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a way of monitoring wherein execution of the application

can be stopped at each of the plurality of remote computers when executing intrusion detection software because it would allow the software to stop execution in the event that an unauthorized object is detected or when time is expired as suggested by **Sprunk** above. One of ordinary skill in the art would have been motivated to do so because it would provide an immediate action response based on which applications or objects are authorized to be executed on each computer system.

4. **Claims 26 and 39-40** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,735,702 to **Yavatkar et al** in view of US Patent 6,842,781 to **Lavian et al** as applied to claims 1-13 and 23 and further in view of US Patent 6,401,238 to **Brown et al.**

As per claim 26, both references disclose the claimed system of claim 23. Neither of the references discloses an intrusion detection server changing the number of said plurality of computers executing intrusion detection software depending on the time of day. **Brown et al** in an analogous art teaches intelligent deploy of application to given machines in a network by a server based on criteria to reflect user needs and network environment (see column 1, lines 40-45). **Brown et al** further discloses determining which of a given set of users (client machines) have a given priority based on a user profile wherein the monitored condition is based on time of day (see column 8, lines 10-11 and 29-30 and abstract) that meets the recitation of an intrusion detection server changing the number of said plurality of computers executing intrusion detection software depending on the time of day. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined

above to include the step of changing the number of said plurality of computers executing intrusion detection software depending on the time of day as suggested by **Brown et al**. One of ordinary skill in the art would have recognized the advantage of providing an intelligent deployment of applications that controls the use of network bandwidth and network priorities as suggested by **Brown et al** (see column 1, lines 26 through column 2, line 25).

As per claim 39, Brown et al discloses applications are initiated at a plurality of remote computers selected based on a number of platforms that are currently active as the server monitors current bandwidth utilization as a measure of traffic over a short period immediately preceding the call to the server that meets the recitation of wherein intrusion detection services axe initiated at a plurality of remote computers selected based on a number of platforms that are currently active (see column 5, lines 40-47 and column 6, lines 39-47). Therefore claim 39 is rejected on the same rationale as the rejection of claim 26 above.

As per claim 40, Brown et al discloses applications are initiated at a plurality of remote computers selected based on network usage to minimize congestion and predetermined rules that take into consideration high and low network usage (see column 6, lines 1-8 and 58-67 and column 1, lines 11-21 and fig. 4) that meets the recitation of wherein intrusion detection services axe initiated at a plurality of remote computers selected based on based on predetermined numbers of maximum and minimum limits on a number intrusion detection platforms (see column 5, lines 40-47 and column 6, lines 39-47). Therefore claim 40 is rejected on the same rationale as the rejection of claim 26 above.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C.C./

Carl Colin
Patent Examiner
September 3, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/4/07